United States Patent [19]

Renaud

[54] **DIGITAL SIGNATURES FOR DATA STREAMS AND DATA ARCHIVES**

[75] Inventor: **Benjamin J. Renaud**, Woodside, Calif.

[73] Assignee: **Sun Microsystems, Inc.**, Palo Alto, Calif.

[*] Notice: This patent issued on a continued prosecution application filed under 37 CFR 1.53(d), and is subject to the twenty year patent term provisions of 35 U.S.C. 154(a)(2).

[21] Appl. No.: 08/753,716

[22] Filed: **Nov. 27, 1996**

[51] Int. Cl.[7] H04L 9/32
[52] U.S. Cl. 713/179; 713/180
[58] Field of Search 380/4, 25

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,405,829	9/1983	Rivest et al.	178/22.1
4,981,370	1/1991	Dziewit et al.	380/25
5,005,200	4/1991	Fischer	380/30
5,031,214	7/1991	Dziewit et al.	380/23
5,163,091	11/1992	Graziano et al.	380/25
5,191,613	3/1993	Graziano et al.	380/25
5,457,746	10/1995	Dolphin	380/4
5,499,294	3/1996	Friedman	380/10
5,572,590	11/1996	Chess	380/4
5,572,673	11/1996	Shurts	395/186
5,619,571	4/1997	Sandstrom et al.	380/4
5,625,693	4/1997	Rohatgi et al.	380/23
5,673,316	9/1997	Auerbach et al.	380/4
5,677,953	10/1997	Dolphin	380/4
5,703,951	12/1997	Dolphin	380/25

5,757,915	5/1998	Ancsmith et al.	380/25

OTHER PUBLICATIONS

"Public–Key Digital Signature Algorithms", Applied Cryptography, 2nd Edition, ISBN 0–471–11709–9.

Cryptolope Containers: A White Paper, downloaded from www.cryptolope.ibm.com/white.htm on Feb. 27, 1997.

Cryptolope Containers in the News, downloaded from www.cryptolope.ibm.com/press.htm on Feb. 27, 1997.

About Cryptolope Containers, downloaded from www.cryptolope.ibm.com/about.htm on Feb. 27, 1997.

Primary Examiner—Tod R. Swann
Assistant Examiner—Todd Jack
Attorney, Agent, or Firm—Beyer & Weaver, LLP

[57] **ABSTRACT**

Methods, apparatuses and products are provided for verifying the authenticity of data within one or more data files. Each data file is provided with an identifier, such as a one-way hash function or cyclic redundancy checksum. A signature file, that includes the identifiers for one or more data files, is provided with a digital signature created with a signature algorithm. The data file(s) and signature file are then transferred, or otherwise provided to a user. The user verifies the digital signature in the signature file using a signature verifying algorithm. Once verified as being authentic, the signature file can be used to verify each of the data files. Verification of the data files can be accomplished by comparing the identifier for each data file with the corresponding identifier in the signature file. If the identifiers in the data and signature files match, then the data file can be marked as authentic. If the identifiers do not match then the data file can be rejected or otherwise dealt with accordingly.

13 Claims, 3 Drawing Sheets